REMARKS

Claims 19-36 are pending in the present application. Applicants have amended independent claims 19 and 27 to include the limitation that "identification is optically read out of optical-diffraction structures of the optical marking." This limitation is not found in the prior art references cited in the pending Office Action and, therefore, distinguishes the present invention from the prior art references cited in the Office Action.

Applicants respond specifically to the issues raised in the Office Action mailed on October 26, 2004 as follows:

Drawings

The applicants have amended Figure 2 and the specification to correct the inconsistencies between the drawings and the specification that were pointed out by the Examiner. A copy of the first sheet of drawings showing Figure 2 with the required amendments is attached.

Claim Objections

Applicants have amended Claim 1 to provide indentations for the limitations. Applicants have amended Claims 27, 28, 33 and 36 to delete the use of the phrases "adapted to" and "adapted for."

Claim Rejections -- 35 USC § 103

Claims 19-36 have been rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 4,442,345 to Mollier et al. ("Mollier" or "the `345 patent") in view of U.S. Patent No.

4,386,266 to Chesarek ("Chesarek" or "the `266 patent") and in view of U.S. Patent No. 6,169,975 to White et al. ("White" or "the `975 patent").

Mollier discloses a method for using a credit card having a non-volatile, erasable memory. This memory has a field for a serial-number, a field for a validating/invalidating character and a field for a key character. Each serial number of all credit cards in a set of credit cards is stored in a memory (3) accessed by a recycling machine (1). Each credit card, when coupled to a holder or reader, is supplied with another key and the key/serial-number correlation is recorded in a disk memory (Fig. 1 and col. 5, lines 22-49).

The serial number is assigned to the credit card (2) during manufacture thereof (col. 8, lines 14-15). The validating character having a predetermined combination of binary zeros and ones, is recorded when all attributes of the credit card which enable identification thereof have been ascertained as being correct during the recycling operation or at the time or original manufacture (col. 8, lines 18-23). If during utilization of the credit card, the key character is modified and no longer corresponds to the key character which was inserted into the memory storage field at the time of manufacture or during the recycling operation, the recycling apparatus recognizes the altered character as being an invalid character and prevents further utilization of the card (col. 8, lines 26 to 35).

Fig. 3 shows details of the non-volatile erasable memory of the credit card. It is a metal nitride oxide semiconductor (MNOS), i.e. all data are stored in a <u>common electronic memory</u>.

Furthermore, none of the data stored in this memory of the credit card disclosed by Mollier is produced as a result of a <u>cryptographic operation</u> with at least two parameters, for example, document-number (serial-number) and a further identification (optically read out of optical diffraction structures of the optical marking). More specifically, Mollier does not disclose nor suggest reading a machine-readable identification out of <u>optical</u> diffraction structures of an optical marking and does not disclose the use of a <u>cryptographic</u> operation.

Chesarek describes a transaction execution system wherein a transaction is authorized based on correspondence of personal identification data entered at a keyboard with account identification data read from an account card. Such systems are used at bank terminals where the customer enters a personal/secret ID number (often a four digit number) for accessing an account. In the use of such systems, the ID number is memorized by the account holder and account data are stored on an account card. Access to is granted if the information on the card corresponds to the ID number.

Chesarek describes the possibility that a key-driven algorithm is provided for determining the relationship between ID number and account number (col. 2, lines 28-30). Encryption keys are maintained in the terminal and used to encrypt the personal data from the credit card for purpose of verification of the personal ID number entered by the consumer (col. 2, lines 54-58). Alternatively, the PIN entered by the consumer is double-encrypted and sent to a host, along with the card data. At the host, the double-encrypted ID number is singly decrypted, the base of the encrypted ID number is accessed, and the encrypted ID number obtained from the data base <u>is compared</u> with the singly <u>encrypted ID number</u> received from the terminal (col. 3, lines 4-19).

None of the systems disclosed by Chesarek uses cryptical optical operations with two different keys. In the second case, an encryption and decryption operation is applied on data, but these data are the PIN number entered by the consumer.

In addition, Chesarek discloses a processing system in which the personal ID data entered at the terminal is encrypted using a first encryption key to give a first resultant. The first resultant is concatenated with a terminal-generated variable number and the terminal uses a second encryption key to generate a double-encrypted personal ID number. The double-encrypted personal ID number is communicated to the host along with the account information data. At the host, the double-encrypted number is decrypted using the second encryption key to yield the first resultant, and the first resultant compared with the validation number associated in the host data base with the account identification data (col. 4, lines 12 to 26). According to this approach, the encryption/decryption process is applied to PIN numbers entered by the consumer, and not to data stored on an account card. Furthermore, the use of the second key is transparent for the verification check that is done by the comparison of the PIN number encrypted by the first encryption key and the validation number associated in the host data base with the account information data (the second encryption key protects the communication over the communication network).

Chesarek does not disclose the use of a first encryption key to generate a check number stored on a document and subsequently applying a cryptographical operation with a second key different from the first key with data read from the document to verify this document.

White is directed to prepaid phone cards. The prepaid phone card contains a PIN number assigned to a prepaid account at the billing system of the phone network operator, which is used to authorize the establishment of calls charged by this account. Such PIN numbers are stored in a sales terminal and printed on a previously blank card along with any other necessary information, i.e. the time, date, sales clerk number, dollar value and time value of the card (col. 2, lines 22 to 45). White also discloses a method which protects access to this terminal wherein an employee has to enter a secret identification code to access the inventory. If a valid code is entered, the employee's ID number is stored with the transaction record so that a complete audit trail of the transaction exists (col. 12, lines 33 to 65).

White does not perform a cryptographical operation on data stored on a document nor generate a check number based on a document number (the prepaid PINs are pre-calculated by the network operator and are totally independent of any card or user information).

Accordingly, none of the references (Mollier, Chesarek and White) cited in the Office Action discloses nor suggests applying an asymmetric cryptographic operation (two different keys) on two or more data stored in machine-readable form on a document. Furthermore, it is an essential feature of the present invention that one parameter is a document number and that the check number produced by the cryptographical operation with the first key is stored on the document.

Optical diffraction structures provide a high level of safeguard against forgery and copying. However, such optical diffraction structures containing machine-readable information can only be manufactured in a cost-efficient manner when produced in large series. An

embossing dye for each diffractive structure has to be incorporated in the document. This is very expensive and can only be cost-efficient if one embossing dye is used for a large number of documents.

The present invention uses <u>two different kinds of information</u> as <u>input parameters</u> of the cryptographical information for the check number stored on the document during the activation process:

- The first information is the machine-readable document number which uniquely identifies the document, but which can easily be falsified and copied.
- The second information is the machine-readable identification read out of the optical diffraction structures of the optical marking, which is difficult to falsify or copy. This information is also difficult to individualize and can only be manufactured in a cost-efficient manner in large series.

By concatenating these different parameters by means of the asymmetric cryptographical operation, it becomes possible to improve the safeguard against forgery or falsification and still enable a cost-efficient manufacturing of the card. This is possible because the document-number already provides information uniquely identifying the document (see, e.g., page 3 of the specification).

Conclusion

Independent claims 19 and 27 have been amended to include the limitation that document identification is optically read out of optical-diffraction structures of the optical marking. None of the cited references (Mollier, Chesarek And White) discloses a method in which the identification that is used is read out of <u>optical diffraction structures</u> of an optical marking together with the document number as input parameters of the cryptographical operation. Therefore, the Applicants submit that the amended claims are not obvious in view of the prior art and respectfully request early allowance of the claims.

Respectfully submitted,

Kevin E. McDermott

Kevin E. McDermott
Registration No.: 35,946
Attorney for Applicants

HOFFMANN & BARON, LLP
6900 Jericho Turnpike
Syosset, New York 11791
(516) 822-3550

196528_1